SW2

FYT Final Report

NFT Security:

Rug Pull Detection

by

Wu Qi

SW2

Advised by

Prof. Shuai WANG

Submitted in partial fulfillment of the requirements for COMP 4981

in the

Department of Computer Science

The Hong Kong University of Science and Technology

2022-2023

Date of submission: April 19, 2023

Table of Contents

1. Introduction

1.1 Overview

The emergence of Non-Fungible Tokens (NFTs) has proposed a new way to trade digital assets are owned and traded. These unique digital assets have created a new asset class that has attracted investors and collectors worldwide. However, with the increasing popularity of

NFTs, concerns have also emerged regarding their security, trustworthiness, etc. In this overview, we will explore the nature, meaning, and limitations of NFTs, as well as their status in the world and Hong Kong society. We will also examine the security issues associated with NFTs, including the concept of Rug Pulls and the importance of rug-pull detection.

1.1.1 What is NFT?

NFT stands for Non-Fungible Token, which is a unique digital asset that is stored on a blockchain and cannot be replicated or duplicated. Unlike cryptocurrencies such as Bitcoin or Ethereum, which are fungible and interchangeable, each NFT is one-of-a-kind. [1]

The mechanism of NFTs is based on blockchain technology, which is a decentralized and transparent digital ledger that records and verifies transactions. NFTs are created using smart contracts with the terms of the agreement between buyer and seller being directly written into lines of code. NFTs can represent various types of digital content, including art, music, videos, and even tweets. Each NFT contains a unique code that verifies its authenticity and ownership.[2]

1.1.2 Why NFTs matter?

The use of blockchain technology and smart contracts enables NFTs to become a new type of asset class with unique properties as it is publicly verified on a blockchain network.

Today, NFTs are used for a variety of purposes, including digital art, music, sports memorabilia, and virtual real estate. [3]

1.1.3. NFT in the Contemporary World

NFTs have gained popularity in the current world and have attracted investors and collectors worldwide. The most common use case for NFTs is the creation and sale of digital art.

Many artists have started using NFTs to sell their digital artwork directly to collectors, bypassing traditional art galleries and auction houses. NFTs have also been used in the gaming industry to represent in-game assets, such as weapons, skins, and characters. [4]

In Hong Kong, the government has recognized the potential of NFTs and blockchain technology to drive innovation and growth in various sectors. On April.9, 2023, Michael WONG from the Financial Secretary Deputy Financial Sector of the Hong Kong Government stated that a series of WEB3 events had been organized in Hong Kong and the government had allocated HK$50 million to Cyberport to expedite the development of the local Web3 ecosystem. [5]

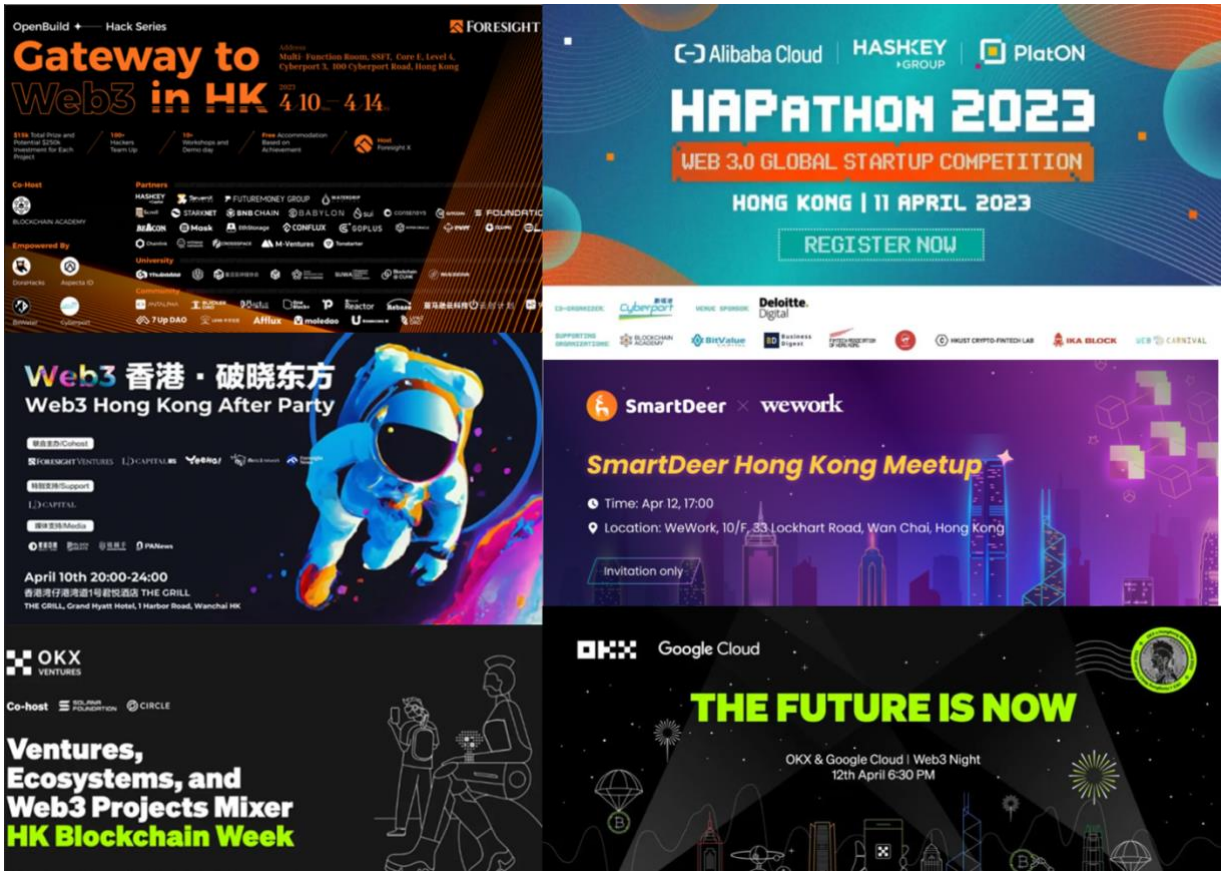

Figure 1.1 A series of WEB3 events in Hong Kong - https://news.marsbit.co/20230404085627412105.html [6]

1.1.7 NFT Security Issues

The rise of NFTs has created a new digital asset class that has captured the attention of investors and collectors alike. However, the security of NFTs has become a major concern for market participants. As per a CoinDesk report [6], the year 2023 has witnessed a new high in cryptocurrency theft with a staggering amount of $119 million being stolen. Notably, NFT collector Kevin Rose lost almost $1 million worth of NFTs when his wallet was compromised in January. Furthermore, according to Crystal's research, there has been a rise in the prevalence of NFT rug pull scams, where founders of projects abscond with users' funds. In the year 2022, 48 such scams were reported, with 41 of them being executed in the latter half of the year.

1.1.8 Rug Pulls in NFT

Rug pulls have become one of the major security issues in the NFT market. This kind of scam happens when developers create a project to make quick profits and then abandon it, leaving investors with worthless tokens. It has stroked a heated discussion such that the US Securities and Exchange Commission has issued warnings to investors regarding Rug Pulls in the NFT market. [7]

Rug Pulls can be classified into two types: soft pulls and hard pulls. A soft-pull rug-pull occurs when the creator of an NFT intentionally devalues the NFT by releasing more copies of the same NFT, diluting its value. A hard pull, on the other hand, occurs when the creator or operator of an NFT marketplace suddenly withdraws all liquidity.

Even NFT trading platforms with large volumes, for example, OpenSea, experience a significant number of rug-pull scams [8]. Among all the rug pulls, the most famous one is Frosties. This collection's Rug Pull cost investors $1.3m [9] and rose the public's awareness of the importance of NFT security.

The consequences of rug pulls can be devastating for investors who may lose their entire investment or suffer significant financial losses. Moreover, these incidents can erode the trust and credibility of the NFT market and discourage new participants from joining, which could undermine the long-term viability of the blockchain ecosystem.

Therefore, we must develop effective mechanisms to detect rug pulls for the investors' information. The rug pulls detection method proposed in this thesis will help address this issue by leveraging advanced algorithms to identify risky NFT projects.

1.2 Objectives

Detecting rug-pull scams has always been challenging, and as we will see in section 1.3, it will be an improvement to have an automatic tool that can tell if a collection is a Rug Pull, given certain features.

The objective of this thesis is to develop a method for detecting rug pulls in NFT collections using supervised machine learning.

This method will collect and analyze metadata and volume data for a wide range of NFT collections. It will also identify indicative features of rug pulls. The model will be trained on a self-established database entailing confirmed Rug-pulls verified by creditable platforms and popular NFT collections.

To achieve this objective, the following steps will be taken:

1.2.1 Search for rug-pulled collections: Research will be conducted to identify NFT collections that are confirmed to be rug pulls.

1.2.2 Collect NFT data: Metadata of popular NFT collections and Rug Pulls will be collected, including attributes such as the collection's name, creator earnings, roadmap information, DAO, and other relevant data such as the total volume for every NFT collection.

1.2.3 Identify indicative features of rug pull: After having analyzed the data, the project will identify the key features that are indicative of a rug pull. Identifying the features will be critical for the machine learning model's importance.

1.2.4 Establish a supervised machine learning model: A supervised machine learning model will be developed and trained on the collected data to identify potential rug pulls in NFT collections.

In summary, this thesis aims to develop a machine learning-based approach for detecting rug pulls on the OpenSea platform. By collecting and analyzing metadata, volume data, and other relevant information for a wide range of collections, the project aims to identify the key features that are indicative of a rug pull. This project also aims at developing a model that can be used to identify potential scams in real time. The resulting methodology will provide a tool for detecting Rug Pull and improving NFT security.

1.3 Literature Survey

1.3.1 'Frosties' – The first Rug-Pull

Frosties [10] is a digital collection of cute, colorful, and ice-cream-scoop-shaped cartoon characters released at 7. Jan 2022 by a couple --- Ethan Nguyen and Andre Llacuna.

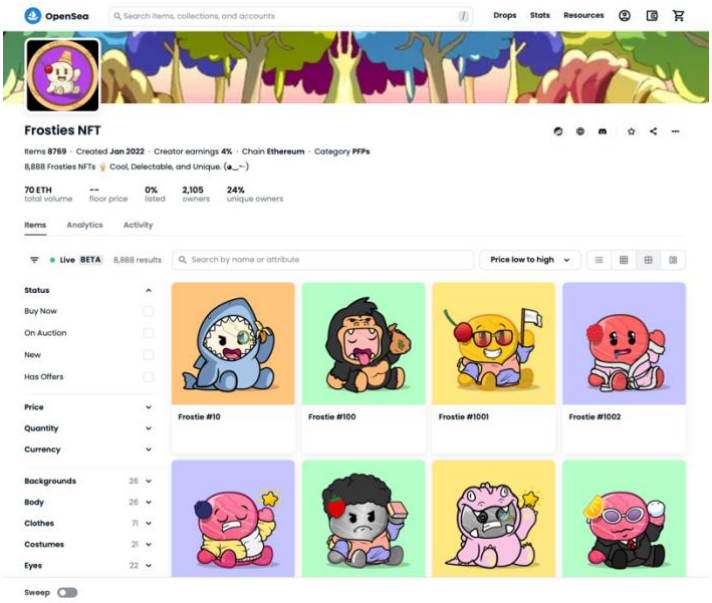

Figure 1 – Frosties NFT, https://opensea.io/collection/frosties-nft [10]

At the first stage of its operation, it was sold at 0.04ETH per mint. The collection sold out within a few hours and earned its creator 335ETH (~ 1 million USD at that time). However, this popular collection didn't promise its holder wealth.

A few hours after the sold-out, the Discord server of the Frosties went down, which made the investors panic. People realized that they have encountered a scam, and this rug-pull was confirmed by Ethan's apology message as well as the deletion of Ethan's Twitter account [11].

The Frosties rug pull had a significant impact on the NFT community, as it was one of the largest and most high-profile cases of a rug pull at the time. It also highlighted the need for better security measures and due diligence in the NFT market, as investors were left to rely on their judgment and research to determine the legitimacy of new projects.

On March 24, 2022, the founders of Frosties were arrested and accused of fraudulent activities [12]. This incident sparked widespread discussion and challenged the NFT community's social trust.

After this incident, some of the victims of Frosties tried to reorganize the Frosties community by placing some of the issued tokens under a new smart contract. In addition to the self-rescue efforts of Frosties holders, OpenSea and other NFT platforms implemented new measures to prevent future incidents. OpenSea, for example, updated its guidelines for listing NFT projects and added new security checks and due diligence processes to verify the legitimacy of new projects. The platform also established a support team to assist investors who were affected by rug pulls or other scams. Besides, the whole NFT community started to notice the new scam and developed appropriate countermeasures and surveillance communities against rug pull. While measures have been taken to prevent future incidents, it is important for investors to remain vigilant and conduct their own research before investing in any new NFT projects.

1.3.2 Rug Pull Finder

The Rug Pull Finder [13] offers a comprehensive database of projects that have been identified as potential rug pulls. The database includes information on the project's contract address, liquidity, and other key metrics. This information is gathered and analyzed by the Rug Pull Finder team, as well as the wider community of investors and analysts. It also collaborates with the Dohd, the Blockchain Intelligence Group, the nfty setup, and vertexbee.com to make joint efforts in clearing up web3. The system's website is displayed below.

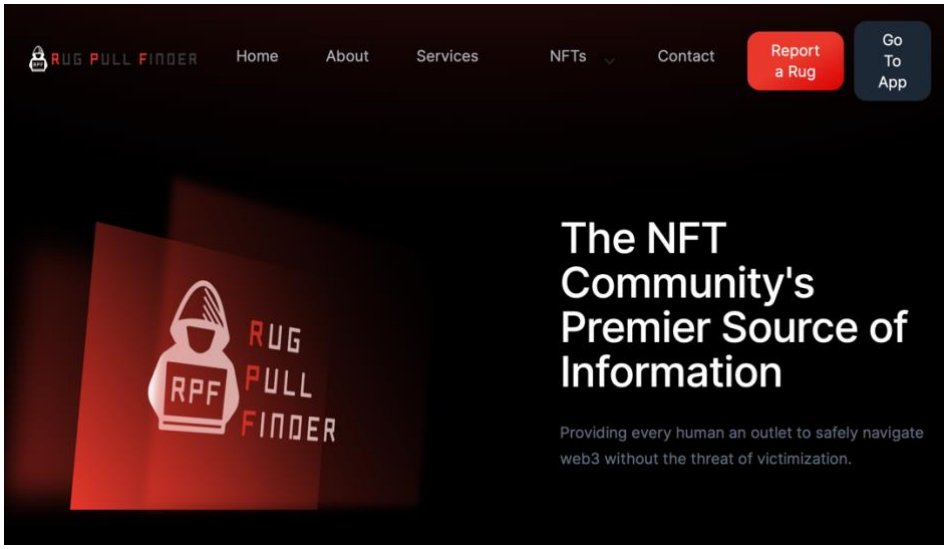

Figure 1.3.1 - The Rug Pull Finder website [13]

The website offers customers a cleaner investing environment and web3 experience by detecting and reporting fraud, thus fostering a community with trust, openness, and surveillance in the web3 world. The company also delivers up-to-date facts on programs, NFT security, and education. Besides, it also provides a community forum where investors can discuss and share information about new projects, allowing for greater collaboration and knowledge-sharing among investors.

Recently, though, it has come to light that the community has fallen victim to a smart contract exploit of smart contract exploit. As reported on September 10 [14], according to RPF, their smart contract had a flaw that allowed one wallet to mint more than one NFT, resulting in 450 NFTs being stolen during the project's free mint stage. After the incident, Rug Pull Finder (RPF) took steps to rectify the situation and recover the lost NFTs. Furthermore, RPF consulted with its online community to ensure that the recovered NFTs were distributed fairly and transparently. The group's response to the incident, including its efforts to recover lost assets and communicate with its community, has been praised by some members of the crypto community.

Despite the incident, Rug Pull Finder has been providing good service and has so far exposed over 15 rug pulls which have stolen more than 40000ETH. [15] Their investigations have also uncovered the involvement of software development agency Omicron Blockchain Solutions in deploying most of these scam projects, as well as the connection between several scam projects through VCs, developers, and even "founders."

Thanks to the Rug Pulls reported by The Rug Pull Finder, the thesis can identify Rug Pulls for training its supervised learning model. And it will use the publicly available data in model training, which will be able to give users instant feedback, inputting metadata of any selected collection.

1.3.3 NANSEN

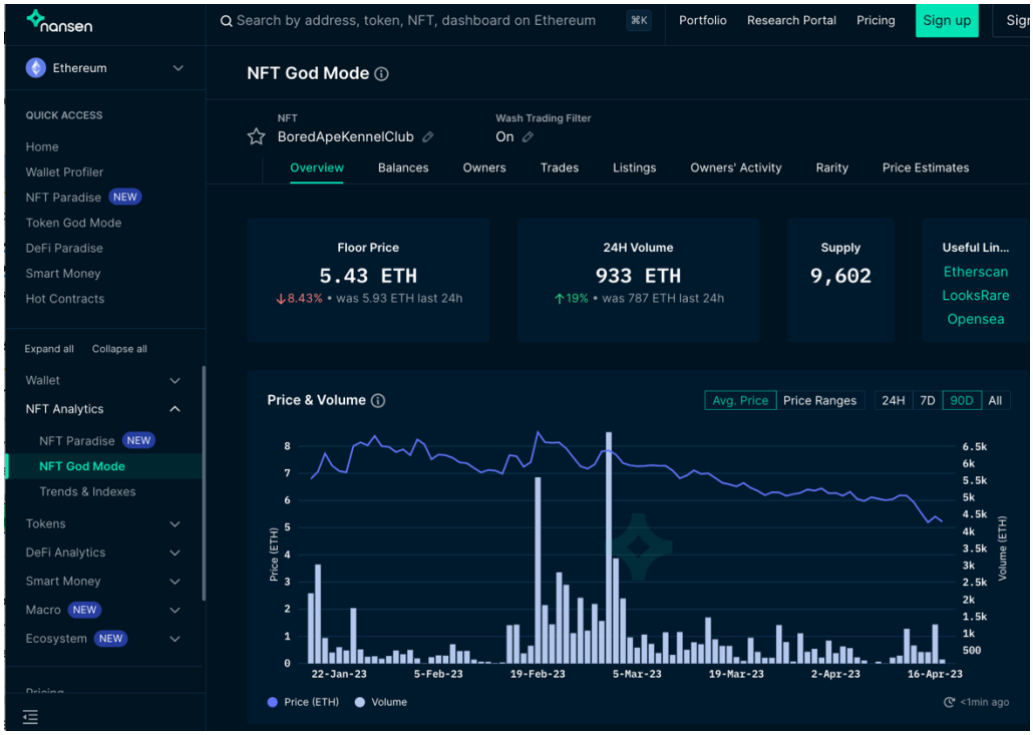

Figure 1.3.2 Nansen website

Nansen is a blockchain analytics platform that provides data-driven insights for the Ethereum network was founded in 2019 by Alex Svanevik and Lars Bakke Krogvig. They intended to provide a comprehensive view of on-chain activity. This website provides insights into transaction flows, smart contract interactions, and token movements. [16]

The platform offers a range of features such as a real-time dashboard, transaction, and address tracking. It has become a powerful tool for researchers to better understand market trends, token holdings, and user behavior on the Ethereum network.

One of the unique features of Nansen is its address clustering algorithm, which helps to identify the real-world entities behind Ethereum addresses. Through an analysis of transaction patterns, Nansen is capable of grouping addresses that are likely owned by the same entity together.

1.3.4 Rug-pull detection on blockchain

The paper "Rug-pull malicious token detection on the blockchain using supervised learning with feature engineering" [17] proposes a supervised learning approach to detect Rug Pull in the cryptocurrency market, especially for blockchains. The authors use feature engineering techniques to extract relevant information from blockchain and identify a set of features as input for their machine-learning models.

The feature engineering process in this paper involves several steps.

First, the authors collect data from the Ethereum blockchain, including transaction data, token data, and price data. They then preprocess this data to filter out irrelevant transactions and tokens. They also calculate several important metrics such as liquidity and trading volume.

Next, the authors produce a set of statistical features based on these metrics. After the feature engineering and model training, the authors use several measuring metrics to determine the performance of the supervised machine learning model. Used ones are the F1-macro score, precision score, and recall score.

Overall, the feature engineering process in this paper has improved the performance of rug-pull scam detection in the cryptocurrency

Group	Item	Description
Token	n_txs	The number of transactions involving the token
	n_addresses	The number of unique addresses involved in transactions
	clus_coefficient	Average over clusters of unique addresses and corresponding transactions value
	total_supply	The number of tokens that have been supplied
Event	n_mint	The number of Mint events
	n_burn	The number of Burn events
	n_transfer	The number of Transfer events
	n_syncs	The number of Sync events
Pool	pool_amount	The amount of wETH in liquidity pool at evaluation point
	w_price	The price converting to wETH at evaluation point
	liquidity	The liquidity of the pool at evaluation point
	tx_curve	HHI at evaluation point of tokens
	liq_curve	HHI at evaluation point of LP tokens
	n_blocks	The number of blocks between token creation and pool creation
	lock	Whether the token has a lock or not (boolean value)
Creator	is_pool_creator	Whether the token creator is pool creator (boolean value)
ABD	n_txs_pb	Average number of transactions per block
	n_addresses_pb	Average number of unique addresses per block
	n_mint_pb	Average number of Mint events per block
	n_burn_pb	Average number of Burn events per block
	n_syncs_pb	Average number of Sync events per block
	transfer_pb	Average number of Transfer events per block
	total_supply_pb	Average number of tokens supplied per block

Figure1.3.3 Features selected by study [17]

market. Having learned the importance of feature engineering, the thesis will also use the necessary method to find features that improve the model performance. Besides, this thesis will also use the F1-macro score, precision score, and recall score to determine the performance of the thesis's machine learning model.

1.3.5 Classic deep learning models

Multilayer Perceptron (MLPs), often used for data classification, consist of layers of perceptron that have activation functions, including fully connected input and output layers and multiple hidden layers. It is widely used to resolve supervised learning problems and can resolve complex non-linear issues while maintaining the same accuracy ratio even with more minor instances [18].

Since relatively few Rug-Pulls have been identified and publicly available, and a collection's interior features may hold unclear connections, MLPs' properties make it a good reference model for our Rug-Pull detection project.

Besides, Radial Basis Function Networks (RBFNs) are another widely used classification model. It compares the input to the training set samples and has a strong tolerance to input noise. RBFNs' single hidden layer design and use of radial basis functions have made it a mighty approximation function [19].

Overall, these DNN models may improve the accuracy of our supervised classification model for Rug-Pull detection. However, it is yet to experiment further whether different types of DNNs will outperform the single-layer models.

2. Methodology

2.1 Design

Having researched the above stated works and more relevant technologies, the thesis has arrived at the following design to detect potential rug pulls:

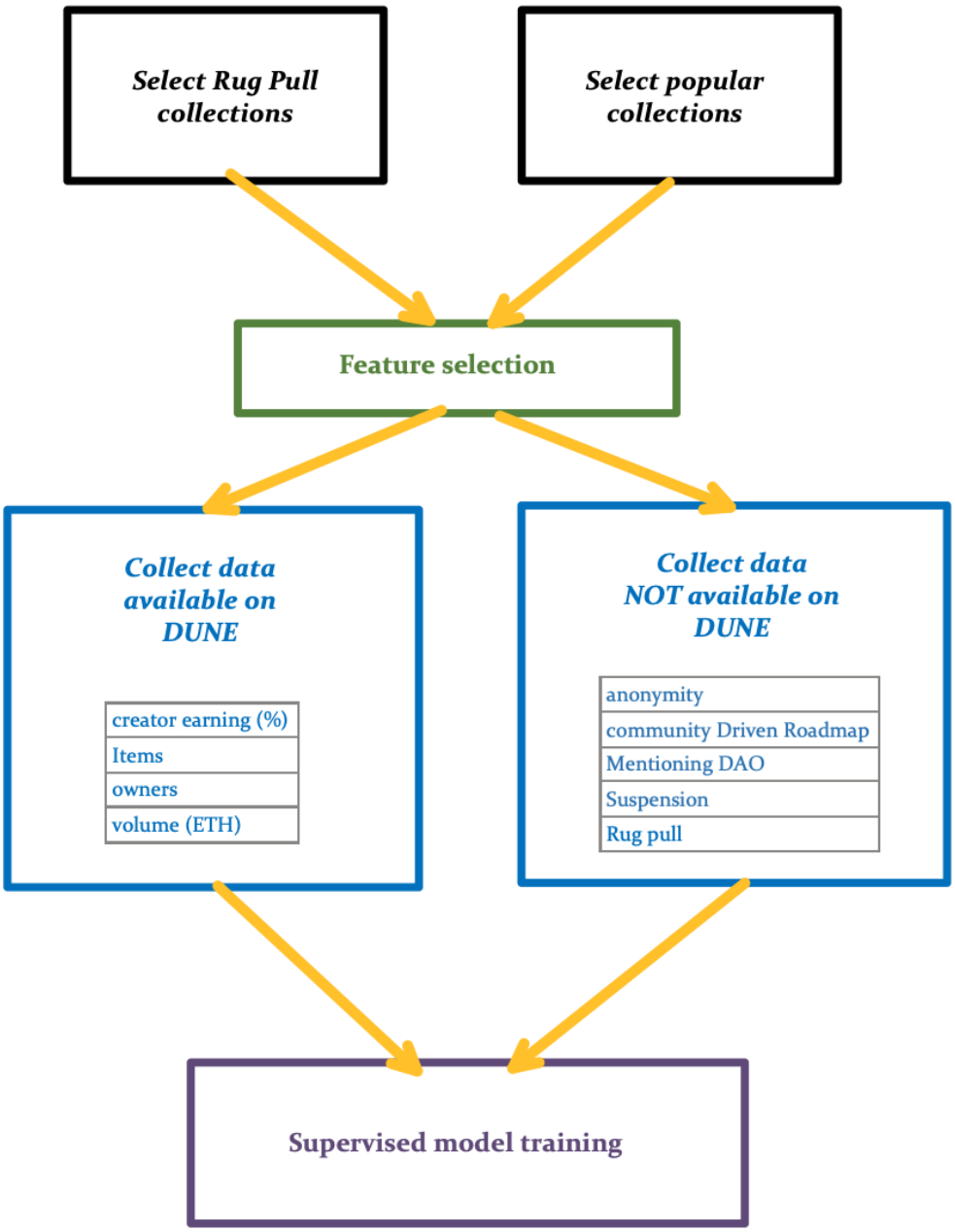

Figure 2.1.1 Design overview

2.1.1 Search for rug-pulled collections

2.1.1.1. Refer to Rug-Pulls reported by Rug Pull Finder

Collect data from Rug Pull Finder on rug-pulled collections.

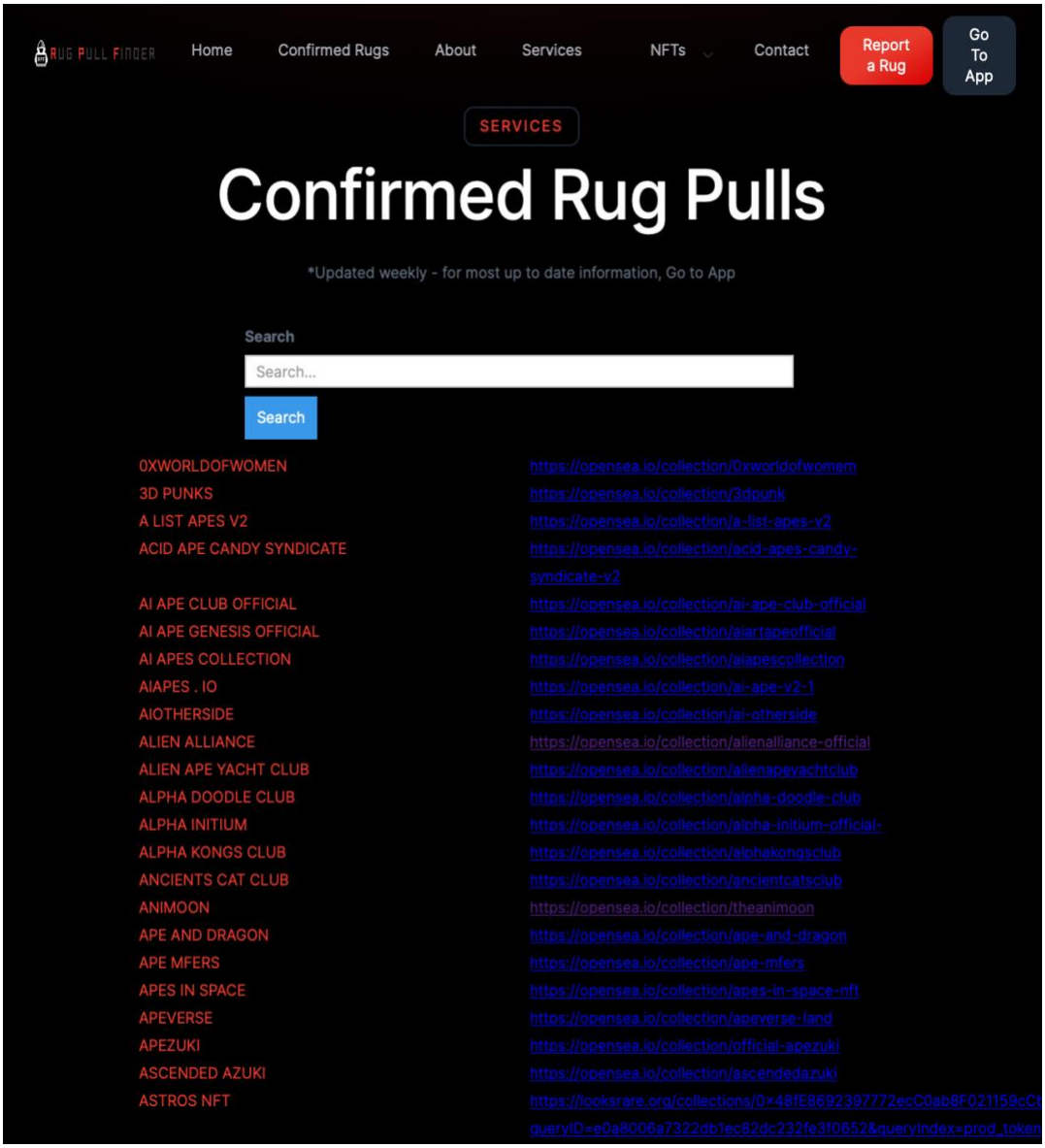

Figure 2.1.2 Part of the confirmed Rug Pulls reported by Rug Pull Finder

2.1.1.2. Refer to Rug-Pulls reported by other authorized platforms.

i) Identify other authorized platforms as sources to confirm Rug Pulls.

ii) Cross-reference the data with the data collected from Rug Pull Finder to increase the accuracy of the detection.

2.1.2. Collect NFT data.

To make the selected data beneficial to most users, this thesis will collect information of the most popular NFT collections on OpenSea.

Why 'popular' and 'OpenSea'?

By popular collections, the thesis is referring to collections that are reported to have large volumes as reported by DUNE on April.3rd. This decision is important for several reasons.

Firstly, it ensures that the data collected is representative of the broader NFT market. This is because collections with a larger volume are likely to be more popular and more widely traded.

Secondly, focusing on popular collections allows for a more comprehensive analysis of the market trends and patterns, since these collections are likely to have a more significant impact on the overall market dynamics. This can help identify potential risks and vulnerabilities in the market. It also helps to mitigate risks for investors and prevent potential losses due to rug-pulls.

Additionally, the thesis chooses to analyze data on OpenSea because OpenSea has a well-developed and accessible API, and their on-chain data is decoded on DUNE for easy data collection and analysis. These decisions simplify the data collection process and reduce the risk of error in the data.

2.1.3 Identify indicative features of Rug Pull

2.1.3.1 Feature Engineering. Feature engineering is an essential step in any data analysis and machine learning process, as specified by 1.3.4, which detailed an example of feature engineering, supervised learning, and Rug-Pulls on the blockchain.

Therefore, we need to carefully select features that are beneficial to the model training.

The following steps have been taken to select measuring features:

i) Research relevant features of an NFT project

2) Identify more critical features by referring to reliable sources

3) Select the relevant features based on the data collected in 2.2.1 and 2.2.2

In this thesis, the features in Figure2.1 are selected:

Group	Item	Description
creator information	anonymity	Whether the NFT creators are hiding their real identities while participating in the market.
community reliance	community Driven Roadmap	Whether the collection is involving its community in the development and direction of the project's roadmap or future plans.
	Mentioning DAO	Whether the NFT collection is acknowledging the use of decentralized autonomous organizations (DAOs) in their governance or decision-making processes.
OpenSea metadata	suspension	Whether the collection is currently removed from a marketplace due to a violation of the platform's rules or terms of service.
	creator earning (%)	The amount of revenue or profit that the creator or creators of a collection earn from the sales of its NFTs on a marketplace.
	Items	the total count of NFTs that have been minted or created and made available for sale within a particular collection on OpenSea
Trading data	owners	the count of unique wallet addresses that hold at least one NFT from a particular collection on a marketplace or blockchain.
	volume (ETH)	Sum of all sales or transactions that have occurred for NFTs within a particular collection on OpenSea. It represents the total value exchanged for the NFTs within that collection.
Rug pull	Rug pull	whether this particular collection or NFT has been confirmed to be a fraudulent project known as Rug Pull

Figure 2.2.1 Features selected to be trained by supervised model.

Why these features?

i) **Anonymity** can be a factor for rug pull as anonymity makes it difficult to identify the people behind the project. Anonymity could potentially enable malicious founders to scam investors without being held accountable. It can also make it harder for investors to conduct due diligence on the project and its creators. It can lead to a higher risk of falling victim to fraudulent schemes. [20]

ii) **Decentralized Autonomous Organization**, or **DAO**, can potentially be an indicative factor of a rug pull in NFT collections. DAO represents a form of decentralized decision-making and governance where stakeholders have voting rights and influence over the direction of the project. A lack of clear or transparent governance mechanisms or a concentration of voting power among a small group of stakeholders can potentially lead to conflicts of interest, and in the worst case, a malicious attempt to deceive investors and conduct a rug pull. Therefore, the thesis decides to make the presence or absence of DAO in a project a factor to consider when evaluating the potential for rug pulls. [21]

iii) **The suspension** of an NFT collection on OpenSea can be an indicative factor of a potential rug pull as it suggests that the collection has violated OpenSea's terms of service or community guidelines, which could be due to fraudulent or malicious activities.

iv) **Creator Earning.** A high creator earning can suggest that the creator may be incentivized to engage in rug pulling or other unethical behaviors, as they have already made a significant profit from the project. In the case of BabyFloki, an identified Rug-Pull, its creator fee was set to 7%, which is higher than usual. It's possible that the high

creator fee is a warning sign that the project is not trustworthy and can potentially become a Rug Pull. Thus, it can be seen as a red flag if the fee is unusually high.

v) **Number of owners** of an NFT collection can be an important factor in detecting potential rug pulls because it can indicate the level of interest and adoption of the collection. Usually, a high number of owners may suggest that the collection has a strong community of supporters who have invested in it, whereas a low number of owners may raise concerns about the legitimacy and popularity of the collection. [22] Additionally, a sudden increase in the number of owners can also indicate a potential rug pull, as it may be an attempt to artificially inflate the value of the collection before a sell-off. However, studying the trend of holders' change is not a focus of this thesis.

By following the above steps, we will be able to build a comprehensive database that will facilitate the detection of rug-pulls in the NFT market.

2.1.3.2 Data preprocessing

The data need to be preprocessed for the upcoming model training. This will involve cleaning the data, handling missing values, and transforming the data into a suitable format for further process. The cleaned and preprocessed data will be split into a training set and a testing set in the later stage.

2.1.4 Establish a supervised machine learning model.

The thesis uses a supervised learning approach to train the model. The model selection process will involve comparing different machine learning algorithms. Once the model is selected, we will train it on the preprocessed data using a suitable machine-learning library. The performance of the trained model will then be evaluated using the testing set on different scorings.

The thesis will use the macro f1-score, precision, and recall, following the evaluation metrics used in the research specified in Section 1.3.4.

Term	Description
TP (True Positive)	The number of actual rug pulls correctly identified as rug pulls by the model. For example, the number of NFTs associated with a rug pull correctly identified as rug pulls.
FP (False Positive)	The number of actual non-rug pulls incorrectly identified as rug pulls by the model. For example, the number of NFTs associated with a legitimate project incorrectly identified as rug pulls.
FN (False Negative)	The number of actual rug pulls incorrectly identified as non-rug pulls by the model. For example, the number of NFTs associated with a rug pull incorrectly identified as legitimate projects.
TN (True Negative)	The number of actual non-rug pulls correctly identified as non-rug pulls by the model. For example, the number of NFTs associated with a legitimate project correctly identified as non-rug pulls.

Figure 2.2.2 (a) TF, TN, FP, FN in the context of Rug Pull detection.

Metric	Description	Formula
Macro f1-score	Primary evaluation metric for imbalanced data	2 * ((Precision * Recall) / (Precision + Recall))
Precision for non-malicious tokens	Proportion of accurate predictions over the total number of predictions made	TP / (TP + FP)
Recall for malicious tokens	Proportion of correctly identified malicious tokens out of the total number of malicious observations	TP / (TP + FN)

Figure 2.2.2 (b) Scoring explained.

2.2 Implementation

2.2.1 Search for rug-pulled collections

2.2.1.1. Refer to Rug-Pulls reported by Rug Pull Finder

Tools: Rug Pull Finder, chrome

2.2.1.1.1. Export to local. The Rug Pull Finder's online Rug Pull list has been exported to a local version of the rug-pull list of rug pulls for faster reference since the website's search engine was found to be broken.

2.2.1.1.2. Selecting Rug Pulls. The Rug Pulls have been deliberately selected to be of different types and of different statuses to reduce potential correlation in features.

2.2.1.1.3. Problems.

i) It should be noted that some projects that were reported as rug pulls had been removed from OpenSea, but their official websites are still running.

ii) Some collections have been confirmed to be a Rug Pull, but there exists another collection with very similar names, which were listed on OpenSea, adding complexity to the process.

iii) Some projects reported as rug pulls by the Rug Pull Finder are not typical Rug Pull. Their founders didn't mean to make the Rug Pull happen, instead, the founders could want to normally run the project but were found to have malicious histories, causing the community to lose faith, thus causing a consequent drop in the value of their project. To make it simpler, these collections are still indexed as rug-pull for the purpose of this study.

2.2.1.2. Refer to Rug-Pulls reported by other authorized platforms.

Tools: Safari, chrome, Firefox. Google, Bing. Twitter, various news websites

2.2.2. Collect NFT data.

Tools: DUNE, Safari

DUNE is a web-based data analysis and visualization platform that allows users to create custom dashboards and queries for data extraction. In the context of the thesis, DUNE is used as a tool for data collection.

2.2.2.1. Refer to existing DUNE dashboards & queries.

Existing DUNE dashboards have been investigated to carry out initial analysis and gain the first data-intensive understanding of OpenSea. The findings have been recorded for future reference.

2.2.2.2. Written custom query on DUNE to extract some of the desired features of popular NFT collections.

Data of features that have been extracted at this step via DUNE:

Total volume

Creator earnings

Number of items

Number of holders

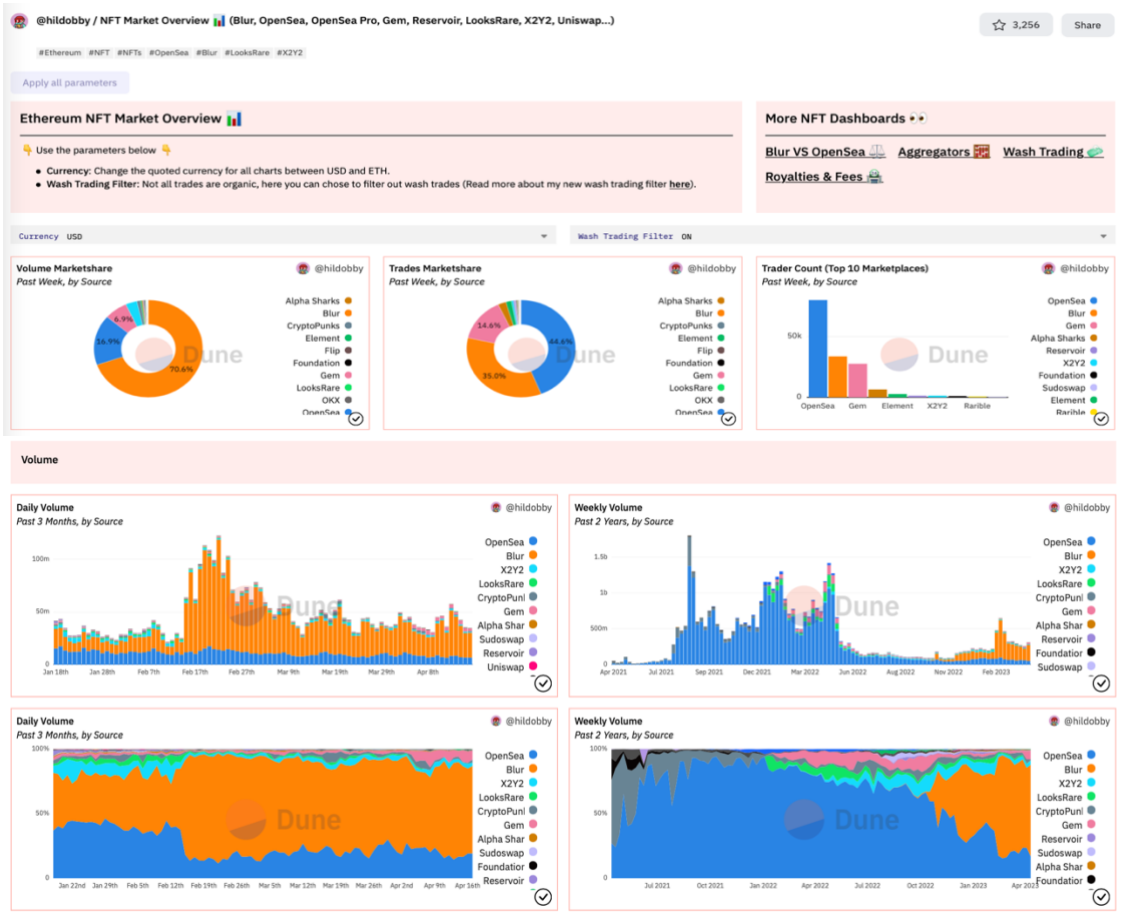

Figure 2.2.3 An example of DUNE dashboard - https://dune.com/hildobby/NFTs [24]

2.2.2.3. Extracted data that are not available on DUNE.

Manual collection

Tools: Safari

Data of features that were extracted manually at this step:

Mentioning DAO

Community Driven Roadmap

Anonymity

Suspended

Rug Pull

i) Mentioning DAO

Approach: Searched for mentions of the collection on collection's official website listed on OpenSea and their recent Twitter activity.

Obstacles: Some collections either had no website or their website had been shut down. Upon encountering the above issue, the data is filled as (-1).

ii) Community-Driven Roadmap

Approach: Researched website roadmaps for information on the collection's development plans

Obstacles: Some collections had no website, some has its website shut down, some has no explicit mention of a roadmap in its website, while some others have deliberately refused to include a roadmap out of branding reasons. Upon encountering the above issue, the data is filled as (-1).

iii) Anonymity

Approach: To determine whether the founder is hiding his or her identity. The implementation process has checked the portfolio posted on OpenSea, whether the Twitter account is verified, whether reliable LinkedIn profiles are linked, if their website has listed their profile, and whether it has been properly registered as a formal company, etc.

Obstacles: Limited by human resources, more comprehensive verification of the founders' identity is required. However, Twitter does not require identity verification for its blue mark, while the nature of NFT determines that the founders do not necessarily need to provide proof of identity.

If the founder's identity is not explicitly stated, the thesis tends to classify it as anonymous (1).

2.2.3 Identify indicative features of Rug Pull

2.2.3.1 Feature Engineering

Please see design: 2.1.3.1 for details

2.2.3.2 Data Preprocess

Tool: Google sheet

The total volume is measured in ETH because in the collected data, each collection's website on Opensea typically displays the total volume in ETH.

Please refer to *Figure2.5* to check the meaning of each cell's numerical value.

	COLLECTION	rug pull	OWNERS	ITEMS	anonymity	communityDrivenRoadmap	mentioningDAO	suspended	creator earning (%)	VOLUME (ETH) (as of 17
2	Bored Ape Yacht Club	-1	5,693	9,998	-1	1	-1	-1	2.5	5185.2435
3	Mutant Ape Yacht Club	-1	11,218	19,465	-1	0	0	-1	2.5	2733.6050
4	CryptoPunks	-1	3,799	9,998	-1	-1	-1	-1	0	601.8915
5	Bored Ape Kennel Club	-1	5,438	9,602	-1	1	-1	-1	2.5	480.7526
6	HV-MTL	-1	10,009	26,398	-1	1	1	-1	5	456.5482
7	Pudgy Penguins	-1	4,616	8,892	-1	-1	-1	-1	5	432.2550
8	CLONE X - X TAKASHI MURA	-1	9,634	19,471	-1	-1	-1	-1	5	369.869
9	Nakamigos	-1	5,674	19,894	-1	-1	-1	-1	5	320.8428
10	Opepen Edition	-1	4,944	15,985	-1	0	0	-1	2.5	246.7335
11	Otherdeed for Otherside	-1	19,753	61,776	-1	-1	-1	-1	5	238.5568
12	Something Official	-1	7,415	19,950	-1	-1	-1	-1	5	226.5200
13	The Captainz	-1	4,639	9,999	-1	1	1	-1	3.33	196.0124
14	Milady Maker	-1	3,311	9,978	-1	-1	-1	-1	5	144.6418
15	NFT Worlds	-1	864	9,999	-1	1	-1.5	-1	9.5	136.7621
16	DeGods	-1	836	8,500	-1	1	1	-1	0.5	129.9847
17	mfers	-1	5,583	10,019	1	0	0	-1	5	113.9417
18	Otherside Koda	-1	3,061	4,996	-1	-1	-1	-1	5	100.0243
19	CyberBrokers	-1	3,135	10,000	-1	-1	-1	-1	5	89.1757
20	Otherdeed Expanded	-1	11,900	37,568	-1	-1	-1	-1	5	87.6848
21	Moonbirds	-1	6,478	10,000	-1	1	1	-1	5	86.688634
22	MeteoriaNFT	-1	1,925	5,998	1	1	1	-1	5.5	85.775549
23	World of Women	-1	5,563	10,000	-1	-1	-1	-1	4	84.3982
24	DEGEN TOONZ COLLECTION	-1	3,787	8,888	-1	0	0	-1	6	84.223018
25	Meebits	-1	6,552	19,999	1	0	0	-1	5	81.9317
26	Spirit Town Official	-1	669	2,023	1	0	0	-1	10	72.831423
27	Whiskers	-1	3,229	5,551	-1	-1	-1	-1	5	64.6833
28	a KID called BEAST	-1	3,746	9,607	-1	-1	-1	-1	5	63.4336
29									5	

Figure 2.2.4 Part of the database data

Feature	Description
Rug pull	-1: not listed as a Rug Pull 1 : has been listed as a Rug Pull
owners	Non-negative value: number of investors holding collection as OpenSea stated -1 : no information available
Items	Non-negative value: number of items in the collection as OpenSea stated -1 : no information available
anonymity	-1: the founders have their identify verified 1: the founder is anonymous 0: information is no longer available
community Driven Roadmap	-1: not explicitly stated / no heavy reliance on community 1 : explicitly stated and has heavy reliance on community 0: no information available
Mentioning DAO	-1: not stated 1 : stated 0 : no information available
suspension	-1: operating 1: suspended
creator earning (%)	Non-negative value: creator earning as stated on their OpenSea website -1 : no information available
volume (ETH)	Non-negative value: the total volume in ETH, as of 17.April -1 : no information available

Figure 2.2.5 Cell value of the database explained.

2.2.3.3 Data Correlation Analysis

Tools: Colab. Python. Libraries: Panda, drive, matplotlib

Link to colab: https://colab.research.google.com/drive/1nyzpXjVQjjbWq5BOC9Mjzx4zoQ_3HsHZ

i) Load data

Data access is granted. On the computer where experiment was carried, Colab can directly load .xlsx from Google Drive.

```
#To read/write data from Google Drive:
#Reference: https://colab.research.google.com/notebooks/io.ipynb#scrollTo=u22w3BFiOveA
from google.colab import drive
drive.mount('/content/drive')

#df = pd.read_excel('/content/drive/My Drive/list.xlsx')
df = pd.read_excel('/content/drive/My Drive/dataN416.xlsx')

# #When done,
# drive.flush_and_unmount()
# print('All changes made in this colab session should now be visible in Drive.')
df
```

Figure 2.2.6 Code -Load data from online Google sheet to colab.

ii) Correlation Plotting

To visualize the correlations between the variables, the thesis has used the Matplotlib library to plot a correlation matrix. This has been achieved by calling the corr() method on the DataFrame and passing the resulting matrix to the matshow() function. The thesis has also labeled the x and y axes of the plot with the column names of the numerical features in the dataset using the select_dtypes() method from pandas library.

```
import matplotlib.pyplot as plt

f = plt.figure(figsize=(19, 15))
plt.matshow(df.corr(), fignum=f.number)
plt.xticks(range(df.select_dtypes(['number']).shape[1]), df.select_dtypes(['number']).columns, fontsize=14, rotation=45)
plt.yticks(range(df.select_dtypes(['number']).shape[1]), df.select_dtypes(['number']).columns, fontsize=14)
cb = plt.colorbar()
cb.ax.tick_params(labelsize=14)
plt.title('Correlation Matrix', fontsize=16);
```

Figure 2.2.7 Code - Plot the correlation matrix.

Two most obvious positive correlations are:

ITEMS – OWNERS

Mentioning DAO – community Driven Roadmap

The positive correlation between mentioning DAO in the collection's website and having a community-driven roadmap suggests that projects that use DAO structures are more likely to involve their communities in the decision-making process and prioritize community input in their development roadmap.

Two weaker positive correlations are:

Anonymity – Mentioning DAO

Rug Pull – suspended.

2.2.4 Establish a supervised machine learning model.

Tools: Colab. Libraries: matplotlib, numpy, panda, drive, sklearn (Ridge classifier, logistic regression, naïve bayes, decision trees, MLP (neural network), and random forests)

2.2.4.1 Model training

Support Vector Machine is selected to be the model for Rug Pull detection.

```
from sklearn.svm import SVC
svm = SVC(kernel='linear', C=1, random_state=42)

svm.fit(X_train, y_train.values.ravel())
svm.predict(X_test), svm.score(X_test, y_test)
```

```
(array([-1, -1,  1, -1, -1, -1, -1, -1, -1, -1,  1, -1, -1, -1,  1, -1, -1,
        -1, -1]),
 0.8947368421052632)
```

Figure 2.2.8 Code – Train SVM model

2.2.4.2 Model Scoring

Scoring and metrics of SVM have also been plotted for further analysis.

```
svm2 = SVC(kernel='linear', C=1, random_state=42)

f1_macroSVM2 = cross_val_score(svm2, X_sc, y_sc, scoring='f1_macro',cv=5)
precisionSVM2 = cross_val_score(svm2, X_sc, y_sc, scoring='precision',cv=5)
recallSVM2 = cross_val_score(svm2, X_sc, y_sc, scoring='recall',cv=5)


f1_macroSVM2, precisionSVM2, recallSVM2
```

Figure 2.2.9 Code – LOOCV and scoring

.

2.3 Testing

2.3. 1 Data Check

The NFT market changes quickly. Therefore, after having collected all data, another data check to update the Rug Pull status and collections' trading data was carried out in April. To double-check the integrity of data, random collections have been selected and the information is double-checked.

2.3.2. Feature Correlation

To test correlation, the correlation matrix is plotted as below.

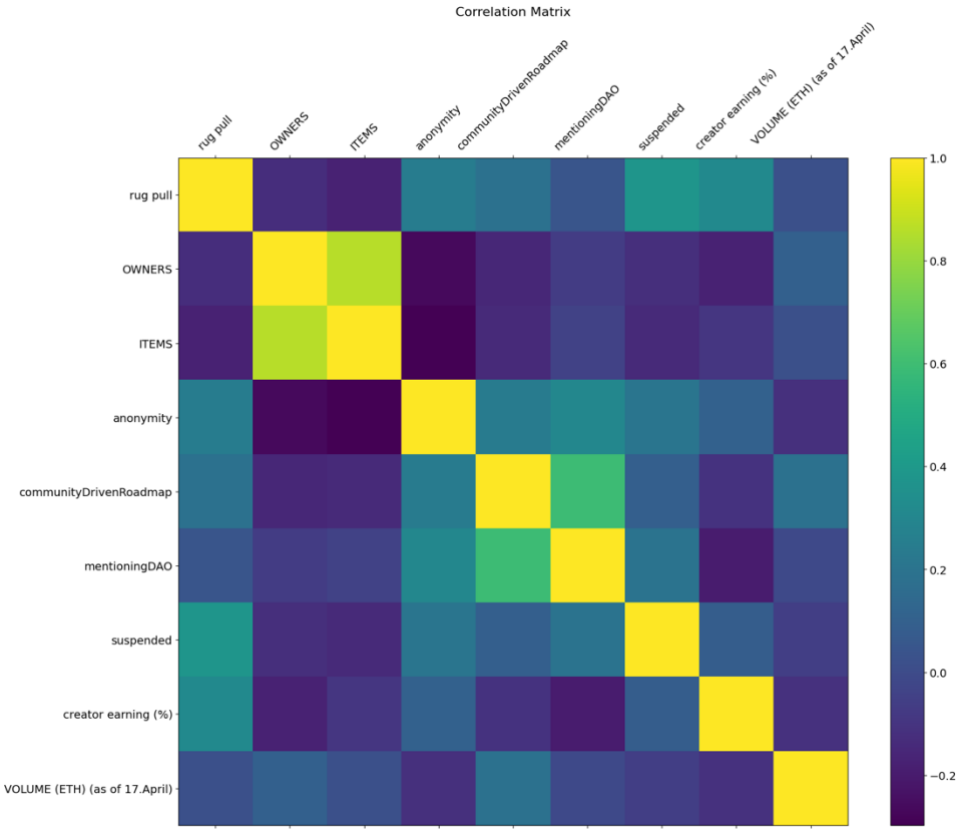

Figure 2.3.1 The correlation matrix

2.3. 3 Model Scoring Comparison

The feasibility of using other models, particularly more complex ones has been tested. These models are classic supervised learning models: Ridge classifier, logistic regression, naïve bayes, decision trees, MLP, and random forests.

Referring to the design section and research introduced in 1.3.4, the six different models has been run on the established dataset using cross validation to avoid overfitting. Considering the size of the thesis's database: CV = 5.

Comparison of mean and variance of their: F1-macro score, precision score and recall score are summarized in a series of bar charts.

MEAN

The **Support Vector Machine** model has the highest mean F1-Macro score (~0.6421)

The **Decision Tree** model has the highest mean precision score (~0.5067)

The **Naïve Bayes** model has the highest recall score (0.8)

VARIANCE

The **MLP** model has the smallest variance in F1-Macro score.

The **Naïve Baye**s model has the smallest variance in precision score.

The **MLP** model has the smallest variance in recall score.

The feasibility of using other models, particularly more complex ones has been tested. These models are classic supervised learning models: Ridge classifier, logistic regression, Naïve Bayes, decision trees, MLP, and random forests.

Referring to the design section and research introduced in 1.3.4, the six different models have been run on the established dataset using cross-validation to avoid overfitting. Considering the size of the thesis's database: CV = 5.

Comparison of mean and variance of their: F1-macro score, precision score, and recall score are summarized in a series of bar charts.

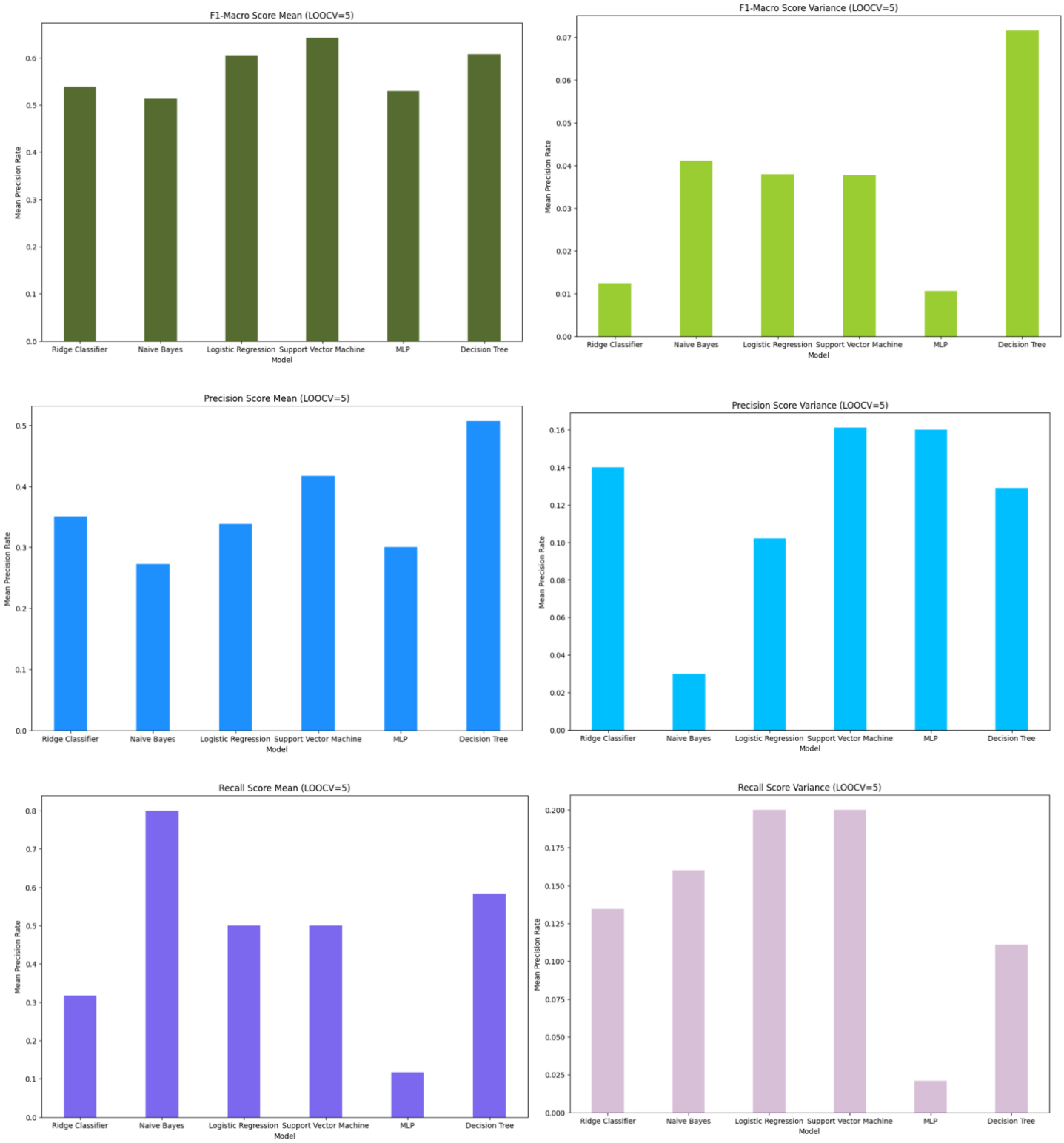

Figure 2.3.2 Graphs plotting F1-Macro, Precision and Recall score for different models.

2.4 Evaluation

2.4.1 Data Collection

i) Problems encountered

Relevant Tools: Google Colab. Python. Libraries: selenium, GeckoDriverManager, Webdriver, chromium-chromedriver, service

The ideal and initially proposed way to scrape data that is not available on DUNE is by implementing an online scrapping tool on colab to achieve a new level of automation. However, most websites need selenium to scrape the full website content, while most tutorials of selenium use the older version and suffer from the same bug as shown in Figure 2.4.1.

However, through manual data collection, details coded in external PDFs can be processed by the human mind. If it were to use web scrapping + phrase detection tools, some important details, specifically mentioning DAO, will be missed.

```
from webdriver_manager.firefox import GeckoDriverManager
from selenium import webdriver

browser = webdriver.Firefox(executable_path=
                GeckoDriverManager().install())
```

```
[WDM] - Downloading: 19.2kB [00:00, 3.27MB/s]
[WDM] - Downloading: 100%|██████████| 2.93M/2.93M [00:00<00:00, 42.2MB/s]
<ipython-input-3-a2d23a8d29fc>:5: DeprecationWarning: executable_path has been deprecated, please pass in a Service object
  browser = webdriver.Firefox(executable_path=
---------------------------------------------------------------------------
WebDriverException                        Traceback (most recent call last)
<ipython-input-3-a2d23a8d29fc> in <cell line: 5>()
      3
      4
----> 5 browser = webdriver.Firefox(executable_path=
      6                 GeckoDriverManager().install())

                                  4 frames
/usr/local/lib/python3.9/dist-packages/selenium/webdriver/remote/errorhandler.py in check_response(self, response)
    243                 alert_text = value["alert"].get("text")
    244             raise exception_class(message, screen, stacktrace, alert_text)  # type: ignore[call-arg]  # mypy is not smart enough here
--> 245         raise exception_class(message, screen, stacktrace)

WebDriverException: Message: Process unexpectedly closed with status 1

SEARCH STACK OVERFLOW
```

Figure 2.4.1 The bug when implementing web scraping on colab with selenium.

ii) Evaluation & Discussion

Overall, the data collection objective is satisfied.

Possible improvements in data collection are to use automatic web scraping tools along with DUNE and build a larger database.

Using automatic web scraping tools along with DUNE for data collection has several potential benefits:

a. By automating the collection process, data can be collected faster and with less human intervention.
b. It could improve the accuracy and completeness of the data collected. Since web scraping tools can collect data from a wider range of sources, they can capture more data points and reduce the risk of human error.
c. By combining it with DUNE and automating the process, we may be able to update our database accordingly automatically.

On the other side, there are also potential drawbacks in using web scraping tools:

a. There may be legal and ethical concerns with using web scraping tools to collect data. Depending on the source of the data, scraping may be prohibited by the website's terms of service or may violate data privacy regulations.
b. The quality of the data collected through web scraping tools may be lower compared to data collected through manual methods. Web scraping tools may encounter technical issues or collect incomplete or inaccurate data.

Further work can be done in building a larger database, with the following benefits:

By increasing the size of the database, more information can be collected and analyzed, which could lead to more accurate and robust conclusions.

However, there are also other aspects to consider before enlarging the database:

Building a larger database may require significant resources and investment, including funding, time, and expertise.

2.4.2 Model Training and feature selection

Evaluation & Discussion

The Support Vector Machine (SVM) model was selected for training in this thesis. The performance of the model has been evaluated based on its accuracy, recall, and training time.

The SVM model achieved an accuracy score of 0. 8947, indicating that the model can correctly identify rug pulls and non-rug pulls with high precision when compared with other models (~0.7). However, the SVM model also exhibited a relatively high variance in the recall score when verified by cross-verification (cv=5), which suggests that the model is not robust enough. It might be attributed to a relatively small dataset size, which affects the generalizability of the model.

In summary, the SVM model shows promise for NFT security and rug pull detection, with an acceptably high accuracy score. However, the model's performance may be limited by the small dataset size used in training, leading to high variance in the recall score.

Additionally, the long training time of SVM models may be a potential drawback in practical applications, making it computationally expensive especially when using large datasets or complex feature engineering techniques.

Future work should focus on addressing these limitations, potentially by increasing the dataset size and exploring more efficient model training techniques.

3. *Project Planning*

Distribution of Work

Task	WU
Carry out literature survey.	●
Collect possible collection data	●
Data collection on DUNE	●
Collect data not available on DUNE	●
Feature Selection	●
Model Review	●
Model training and Selection	●
Data Analysis	●
Evaluation	●

● Leader

GANTT Chart

Task	July	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
Carry out literature survey.										
Collect possible collection data										
Data collection on DUNE										
Collect data not available on DUNE										
Feature Selection										
Model Review										
Model training and Selection										
Data Analysis										
Evaluation										

4. Required Hardware & Software

Hardware

Development PC:	MacBook Air with 1.6GHz double Intel Core i5
Minimum Display Resolution:	2560 * 1600 with 16-bit color

Software

Python, SQL	Programming languages
Google colab, DUNE	Development platforms

5. References

[1] “What is a non-fungible token (NFT)? your ultimate guide,” OpenSea. [Online]. Available: https://opensea.io/learn/what-are-nfts. [Accessed: 10-Apr-2023].

[2] “What is Ethereum?” ethereum.org. [Online]. Available: https://ethereum.org/en/what-is-ethereum/. [Accessed: 10-Apr-2023].

[3] Y. Gupta, J. Kumar, and D. A. Reifers, “Identifying security risks in NFT platforms,” arXiv.org, 05-Apr-2022. [Online]. Available: https://arxiv.org/abs/2204.01487. [Accessed: 10-Apr-2023].

[4] K. Pineda, “Magic Eden bets on NFTS to disrupt gaming industry despite gamers' skepticism: Hot forex signals,” Hot Forex Signals, 30-Sep-2022. [Online]. Available: https://hotforexsignals.com/magic-eden-bets-on-nfts-to-disrupt-gaming-industry-despite-gamers-skepticism/. [Accessed: 10-Apr-2023].

[5] M. WONG, “Blog,” Financial Secretary - My Blog - Developing Web3 with innovation and steadiness. [Online]. Available: https://www.fso.gov.hk/eng/blog/blog20230409.htm. [Accessed: 10-Apr-2023].

[6]“香港 4 月份 web3 活动汇总_marsbit,” Mars Finance. [Online]. Available: https://news.marsbit.cc/20230404085627412105.html. [Accessed: 15-Apr-2023].

[7] A. Baydakova, “$119m in stolen crypto so far in 2023, NFT rug pulls on the rise: Crystal Blockchain,” CoinDesk Latest Headlines RSS, 24-Mar-2023. [Online]. Available: https://www.coindesk.com/consensus-magazine/2023/03/24/119m-in-stolen-crypto-so-far-in-2023-nft-rug-pulls-on-the-rise-crystal-blockchain/. [Accessed: 10-Apr-2023].

[8] “Justice Department Announces Enforcement Action Charging Six individuals with cryptocurrency fraud offenses in cases involving over $100 million in intended losses,” The United States Department of Justice, 30-Jun-2022. [Online]. Available: https://www.justice.gov/opa/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency-fraud. [Accessed: 10-Apr-2023].

[9] P. Banerjee, “Beware of rug pulls while dealing in nfts; here's what it means and how you spot,” mint, 12-Jan-2022. [Online]. Available: https://www.livemint.com/technology/beware-of-rug-pulls-while-dealing-in-nfts-here-s-what-it-means-and-how-you-spot-11642014485169.html. [Accessed: 10-Apr-2023].

[10] “NFT rug pull leaves investors $1.3m out of pocket” Yahoo! Finance, 11-Jan-2022. [Online]. Available: https://finance.yahoo.com/news/nft-rug-pull-leaves-investors-025838856.html. [Accessed: 10-Apr-2023].

[11] OpenSea, “Frosties NFT - Collection,” OpenSea. [Online]. Available: https://opensea.io/collection/frosties-nft. [Accessed: 13-Feb-2023].

[12] B. Pimentel, “Anatomy of an NFT art scam: How the frosties rug pull went down,” Protocol, 25-Feb-2022. [Online]. Available: https://www.protocol.com/fintech/frosties-nft-rug-pull. [Accessed: 13-Feb-2023].

[13] Two Defendants Charged in Non-Fungible Token (“NFT”) Fraud and Money Laundering Scheme. 2022.

[14] Rug Pull Finder. [Online]. Available: https://www.rugpullfinder.io/services. [Accessed: 13-Feb-2023].

[15] S. T. U. T. I. MANSATA, “Rug pull finder falls victim to Smart Contract Exploit,” The Crypto Times, 05-Sep-2022. [Online]. Available: https://www.cryptotimes.io/rug-pull-finder-falls-victim-to-smart-contract-exploit/. [Accessed: 10-Apr-2023].

[16] C. Tan, “Rug pull finder exposes over 15 NFT scams that have stolen over 40,000 ETH,” NFTgators, 13-Apr-2022. [Online]. Available: https://www.nftgators.com/rug-pull-finder-exposes-over-15-nft-scams-that-have-stolen-over-40000-eth/. [Accessed: 10-Apr-2023].

[17] “About us: Who are we?” Nansen. [Online]. Available: https://www.nansen.ai/about. [Accessed: 10-Apr-2023].

[18] M. H. Nguyen, P. D. Huynh, S. H. Dau, and X. Li, “Rug-pull malicious token detection on blockchain using supervised learning with feature engineering: Proceedings of the 2023 Australasian Computer Science Week,” ACM Association for Computing Machinery, 01-Jan-2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3579375.3579385. [Accessed: 10-Apr-2023].

[19] "How Do Multilayer Perceptrons Help Solve Complex Problems?" H2O.ai. https://h2o.ai/wiki/multilayer-perceptron/(accessed Feb. 13, 2023).

[20] Principle of Neural Network and Its Main Types: Review - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/The-Main-Advantages-and-Disadvantages-of-the-RBF_tbl3_343837591 [accessed 13 Feb 2023]

[21] D. Das, P. Bose, N. Ruaro, C. Kruegel , and G. Vigna, “Understanding security issues in the NFT ecosystem: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security,” ACM Conferences, 01-Nov-2022. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3548606.3559342. [Accessed: 10-Apr-2023].

[22] C. Bellavitis, C. Fisch, and P. P. Momtaz, “The rise of Decentralized Autonomous Organizations (DAOs): A first empirical glimpse,” SSRN, 11-May-2022. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4074833. [Accessed: 12-Apr-2023].

[23] Y. Gupta, J. Kumar, and D. A. Reifers, “Identifying security risks in NFT platforms,” arXiv.org, 05-Apr-2022. [Online]. Available: https://arxiv.org/abs/2204.01487. [Accessed: 12-Apr-2023].

[24] @hildobby, “NFT market overview (Blur, OpenSea, OpenSea Pro, gem ... - dune,” DUNE. [Online]. Available: https://dune.com/hildobby/NFTs. [Accessed: 15-Apr-2023].

Appendix A: Meeting Minutes

Minutes of the 1st Project Meeting

Date: June 23, 2022
Time: 3:45 pm
Place: Huddle, SLACK
Present: prof. Shuai WANG, Dr. Zonjie LEE, Qi WU
Absent: None

1. Report on progress
   1.1 Introductory knowledge of NFT acquired.
2. Discussion items
   2.1 Determined the theme for the upcoming FYT project to be centered on NFT security.
   2.2 Introduction to the different type of rug pulls.
   2.3 possible solutions using machine learning approach for predicting future rug-pull NFT projects.
3. Goals for the coming week
   3.1 future investigation into the topics of NFT security
4. Meeting adjournment and next meeting
   The meeting was adjourned at around 4:30 pm

Minutes of the 2nd Project Meeting

Date: Oct 13, 2022
Time: 3:00 pm
Place: Huddle, SLACK
Present: Prof. Shuai WANG, Dr. Zongjie LI, Qi WU

1.Report on Progress
   1. 1 report on data collection process
   1.2 report on DUNE query, DUNE codes:< floki, NFT ranking , test1>
2.Plan for the coming week

Minutes of the 3rd Project Meeting

Date: Oct 27, 2022
Time: 3:00 pm
Place: Huddle, SLACK
Present: Prof. Shuai WANG, Dr. Zongjie LI, Qi WU

1.Report on Progress

1. 1 report on data collection process

1.2 report on DUNE query, DUNE codes:< floki, NFT ranking , test1>

2.Plan for the coming week